LA-UR-22-22769

Approved for public release; distribution is unlimited.

Title: Progress Report for the Pathfinder Project: A Laser-Based / Fiber Optic IAEA Seal that Implements Spectral Interferometry

Author(s): Pickrell, Mark Manley
Gilbertson, Steve Michael

Intended for: Report

Issued: 2022-03-25

Los Alamos
NATIONAL LABORATORY

Los Alamos NATIONAL LABORATORY

NNSA National Nuclear Security Administration

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Progress Report for the Pathfinder Project: A Laser-Based / Fiber Optic IAEA Seal That Implements Spectral Interferometry

Mark M. Pickrell, Steve Gilbertson, J-4

February 18, 2021

I. Bottom Line Up Front

We have completed the system design for this seal, which is documented here. We have also built a bench-top test of this system and demonstrated that it works. Data are presented here. Moreover, we have demonstrated a precision of 25 microns using just our available parts. With a proper spectrometer, the detection sensitivity would be about 10 microns, or 1/8th the size of a human hair. This resolution is about 100 - 300 times smaller than the best available technology for splicing telecommunications, single-mode fiber.

II. Detailed Report

This is the first progress report for the Laser / Fiber-Optic Based IAEA Seal. This seal implements spectral interferometry, which is crucial for its resilience to tampering. Indeed, based on our understanding of telecommunications-based fiber optic technology, it is essentially impossible to tamper with the fiber without detection either immediately (with an active system) or subsequently (with a passive system).

Recall that the significance of the spectral interferometry method is that the tamper indication is not simply the transmission of light, but rather the spectral interferogram of two separate laser pulses. This interferogram is unique to a pair of fibers, and even the smallest length change in either fiber will significantly affect the measurement. This phenomenon is somewhat non-intuitive, and that aspect is one reason why the seal is exceedingly tamper resistant. The common understanding of interferometry is in the time domain; as waves vary in phase there are fringes in time. However, this design has interference in the wavelength domain, not the time domain, and is a consequence of wave mechanics. Our initial tests show that a simple, modestly-priced system will have a length detection sensitivity of 10 microns. The width of a single human hair is (on average) eight times larger at 80 microns. There is simply no extant technology that can cut and re-splice a telecommunications, 9 micron fiber accurate to 10 microns. Indeed, current technology might be able to splice accurate from 100 to 300 times that, or 1 – 3 millimeters.

The physics basis of the spectral interferometry method is that the Fourier Transform of a short, Gaussian, laser pulse has a wavelength (frequency) spectrum that is also a Gaussian (un-normalized):

$$\Im\left[e^{\frac{-t^2}{2\tau^2}}\right]\Rightarrow e^{\frac{-(\omega-\omega_o)^2}{2\sigma^2}}=e^{\frac{-(\lambda-\lambda_o)^2}{2(\Delta\lambda)^2}} \qquad (1)$$

The significance here is that the Gaussian width in time is related to the Gaussian spectral width in wavelength (frequency) by:

$$\sigma = {}^{1}\!/_{\tau}$$
$$\Delta\lambda = \frac{\lambda_o^2}{c\tau} \tag{2}$$

Thus, a short laser pulse has a wavelength spectrum that is spread out, and, the shorter the pulse in time, the wider the wavelength spectrum. It is a phenomenon of wave mechanics that the short-time pulse of a laser will produce a broad spectrum, and that broad spectrum can easily be recorded on a spectrometer. If two short time pulses are produced that are relatively close together, but are not overlapping, they will combine and interfere in the spectral domain. (“Relatively close together” is determined by the wavelength resolution of the spectrometer.) The reason is that the Fourier components extend well beyond the pulses in time, (mathematically they extend to infinity). The reason for the spectral interference is the phase difference of the Fourier components of the two pulses. The phase delay depends on the laser light frequency, ω, (within the spectrum) and the time difference between the two pulses Δt :

$$\Delta\phi_\omega = \omega\Delta t \tag{3}$$

This effect is shown in Figure 1 below.

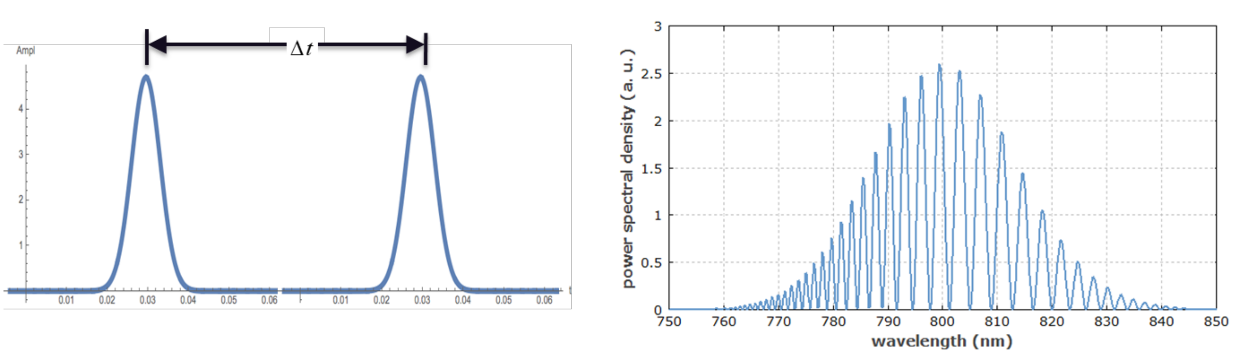

Figure 1: Two short-time laser pulses on left separated in time. The resulting spectral interference pattern on right.

An effective method for creating two closely-spaced, short-time, laser pulses is to use a pulsed laser and the standard Michelson interferometry topology, implemented using fiber optics. That is the basis for this seal technology. The spectral interference pattern shown in Figure 1 above is unique to the difference in optical length between the reference and measurement legs of the fiber interferometer. The significance is that the interference pattern can detect perturbations on the order of 10 microns (we have already demonstrated our system to 25 microns). Therefore, any attempt at splicing or damaging the fiber would be detectable if the optical length changed by as little as 10 microns.

We envision three variants of this seal, depending on the protection requirements:

1. A fully active seal, so that the fiber is interrogated at the pulse frequency of the laser. The nominal laser pulse rate is 100 MHz, so that the time for detection of any tampering would be on the order of 10 nanoseconds. However, a more practical limit would be the time to download a spectrum from the spectrometer, which is about 1millisecond. That spectrum would therefore consist of 100,000 averaged interference spectra.

2. An active seal that is switched between individual canisters. An example would be a spent-fuel storage vault. Each storage container would have part of the seal (a relatively inexpensive part), and a central system would optically switch between seals. The nominal detection time for any tampering would be on the order of a few minutes.
3. A passive seal that would be subsequently interrogated by the laser/spectrometer/computer test system. We will describe the safeguards to make this system effective. It has the benefit that each seal would be very inexpensive, probably on the order of a few hundred dollars.

The system design of each of these variants will be discussed at length in this report. We start with the active seal because it is easier to explain the overall operation of the fiber-optic, spectral interference seal approach in this context. The active seal design is shown below in Figure 2.

A. Active Seal

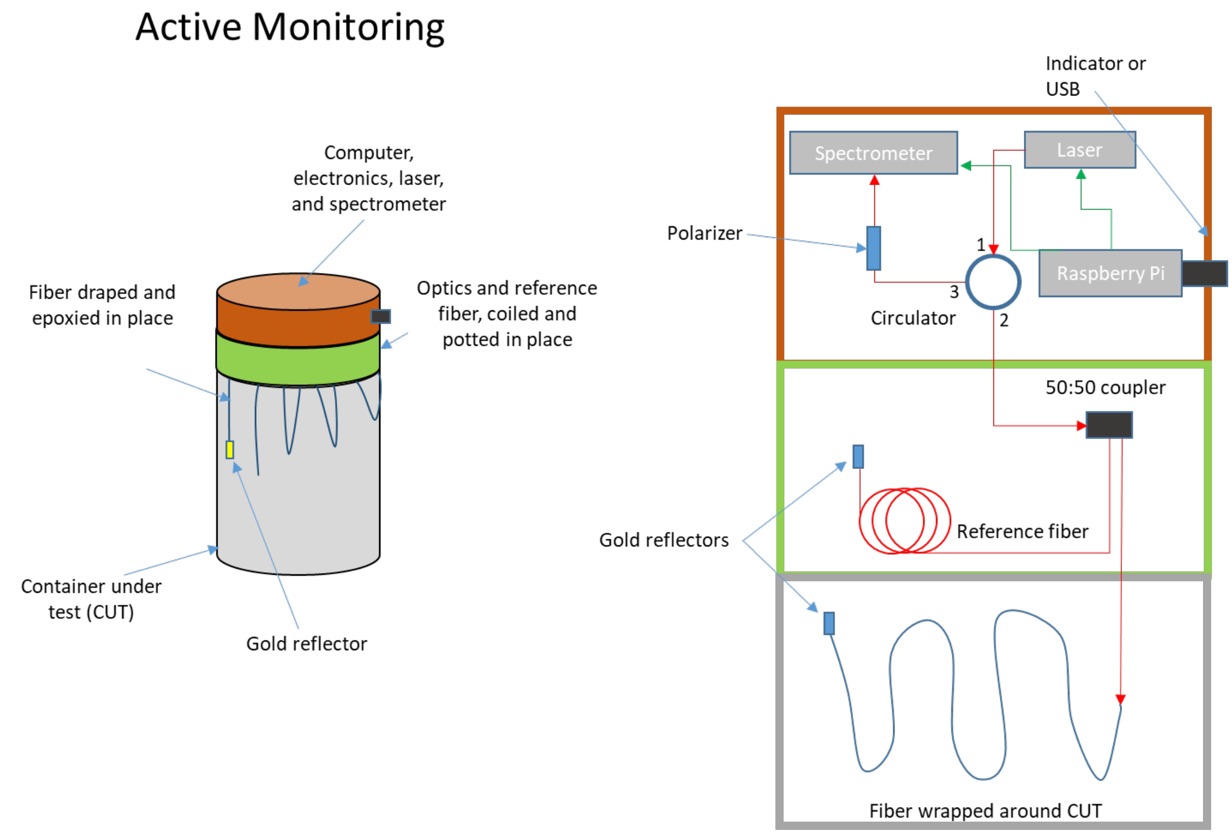

Figure 2: Optical topology and system electronics for a fully active, fiber optic, spectral interference seal. Note that the grey cylinder is the container under test. The brown and green vessels are really a single integrated container; the color coding is used to indicate different functionality only. Some details such as a battery and split transformer power connection are omitted. We emphasize that the spectral interferometry technique measures the optical length difference of the two fibers, thus the Reference fiber can act equally effectively as a detector as the test fiber. Although not depicted in this picture, the reference fiber would be wrapped around the inside of the electronics and optical container and epoxied in place. It would prevent tampering with the optical and electronic components.

The system schematic shown above in Figure 2 shows all of the essential components of the spectral interferometry seal, with the exception of the encrypted optical switch, which applies only to the switched active and passive seal variants. It will be discussed later in this report. For the full active seal shown above in Figure 2, the brown and green enclosures are really a single, integrated enclosure. The color coding is meant to distinguish functionality only. The system is controlled by a credit-card computer, such as a Raspberry Pi. (In a demonstration unit, we will use a laptop instead). The computer controls the pulsed laser and the spectrometer. It also provides a status output that will be optical only, so that there is no mechanism for electrically interfering with the seal operation.

The laser produces short pulses on the order of 90 femtoseconds (90 fs) each. The repetition rate is adjusted to a nominal rate of 100 MHz, so that a separate reading is made every 10 ns. The nominal full width, half-maximum of the wavelength spread is 50 nm. A single pulse enters port one of the circulator and exits port 2. It is split into two separate pulses at the 50:50 coupler, and each of these pulses travels down the respective fibers (the test fiber and the reference fiber). Each pulse is reflected by a gold reflector at the cable end and travels back along the fiber. The pulses are recombined at the 50:50 coupler and enter port 2 of the circulator. The two pulses, now separated in time by, perhaps, 100 fs, exit port 3 of the circulator, are selected for a single polarization, and are measured by the optical spectrometer. The wavelength interference occurs because of the recombination of the pulses in the coupler. The computer downloads the spectrum from the spectrometer and performs a Fast Fourier Transform (FFT) on the data. Multiple pulses can easily be averaged to improve precision and sensitivity.

An essential aspect of the spectral interferometry technique is that it measures the difference in length between two fibers, in this case the reference and test fibers. It does not measure an absolute length. The fibers can essentially be any length (subject to excessive light loss), but the two fibers must be nearly the same length, limited by the resolution of the spectrometer, (about 1 cm.). The significance is that the two fibers are essentially interchangeable; the system detects the change in transmission length for either of them. Therefore, the construction design has the reference fiber wrapped around the inside of the entire electronics and optical package, and epoxied in place. The epoxy will also seal the optics and electronics package, so that any attempt at tampering would also be detected by the damage to the reference fiber.

We have assembled a bench-top test apparatus of this system, with all components except the encrypted optical switch. The setup is shown below in Figure 3. We emphasize that we used parts we had available; we did not use parts specifically selected for this application. That will be the next step, and we would anticipate improved performance as a consequence.

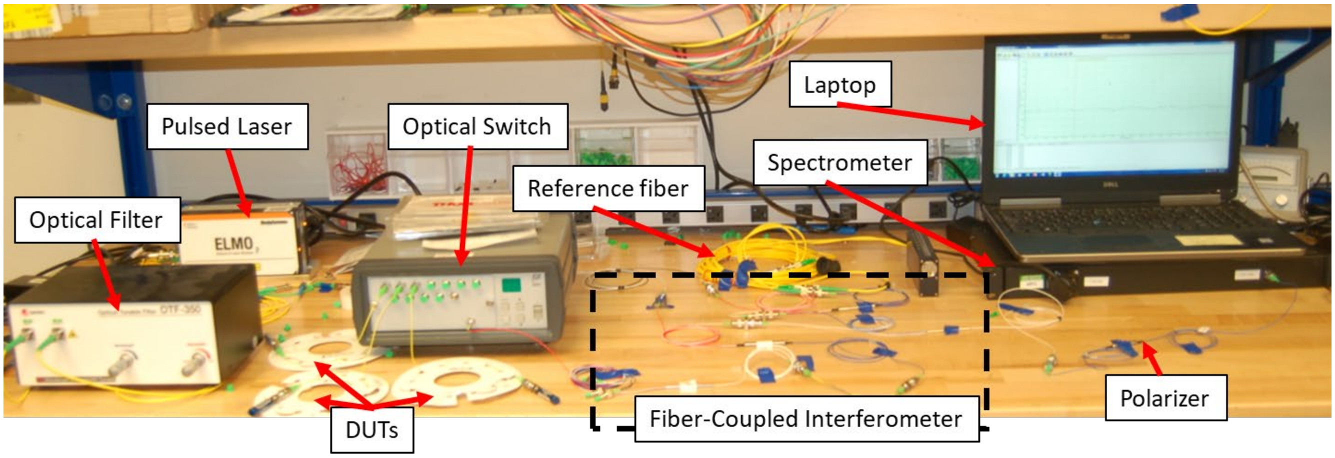

Figure 3: Picture showing the bench top test of the spectral interferometry seal. All components are labeled. The only component not used is the encrypted optical switch, which is not needed to demonstrate the performance. Also note that this setup actually implements the switched active seal discussed in section III below, but we can select a single fiber to test the purely active configuration.

The results using this system are shown below in Figure 4. This shows the snapshot of a single laser pulse, however, the system runs continuously at the laser pulse frequency. The upper trace is a spectrum and shows the nominal interference pattern. The lower trace shows a single FFT analysis, which is the optical path length difference between the two fibers. The computer downloads the spectrum as quickly as the spectrometer will allow, which is nominally 1 kHz (1 millisecond per spectrum). Each downloaded spectrum consists of the spectral average of about 100,000 laser pulses. Then, in real time, the computer performs the FFT on the downloaded spectrum which provides the measurement of the fiber length difference. Multiple measurements of the length measurement can then be averaged for improved resolution. A complete measurement could take a mere 1 second, which would be the average of 1,000 FFT-reduced length measurements and 100 million laser pulses.

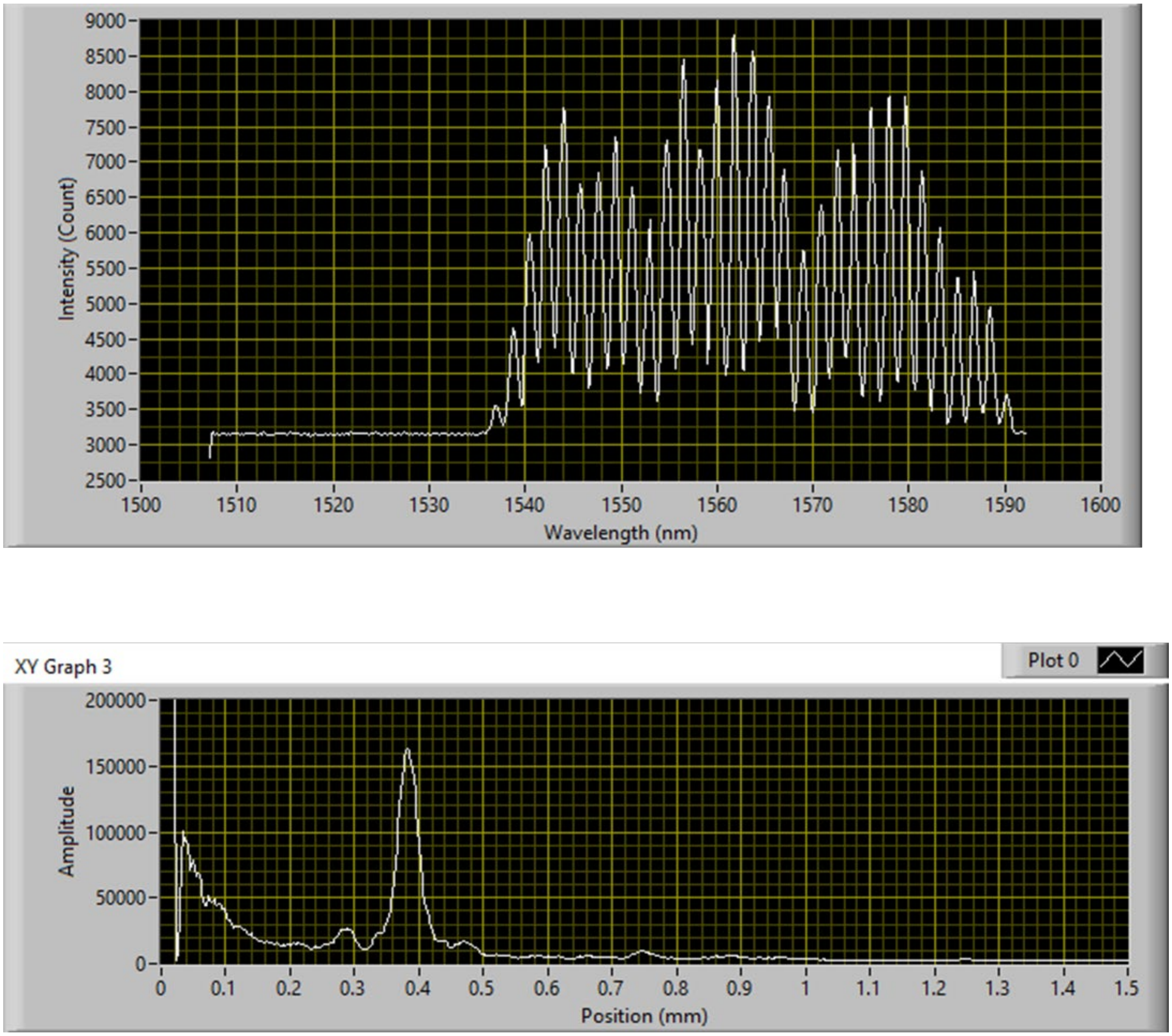

Figure 4: Results from our initial tests using the bench-top system. These traces are a snapshot from the system; they show the measurement from a single laser pulse. The upper trace shows the raw spectrum, and the spectral interference is clear (compare to the theoretical prediction in Figure 1 above). The lower trace is the FFT analysis of the spectrum, and shows the optical length difference between the test and reference fibers. Note that the small divisions of the position correspond to 25 microns, which is the nominal precision of the system.

1. Initial Vulnerability Assessment for This Configuration

We now consider a very preliminary assessment of the vulnerability of this system to possible tampering. Several scenarios will be addressed. This is intended to be descriptive, not a formal Vulnerability Assessment. Some of the possible scenarios are:

- The attacker cuts the test fiber in two places and removes the protected component. Then, the attacker re-splices both fiber cuts. This scenario is virtually impossible to complete. The entire process would have to be done in 10 microseconds. The fiber cuts would have to have no effect on the length of the fiber, at least at the level of 10 microns. No fiber splicing technology has this ability. The fiber splices would have to have almost no lost material, and the splicing would have to maintain the fiber diameter exactly, otherwise the fiber length would change.
- The attacker cuts the container holding the item in between two fiber wraps. This method would be easy to prevent merely by wrapping the test fiber closely enough that no viable access were possible.
- The attacker attempts to disable the seal by cutting into the electronics and optical enclosure. This method would fail because the enclosure is protected by the reference fiber, and both the enclosure and the fiber are sealed with epoxy. Attempting to open the enclosure would destroy the reference fiber.
- The attacker attempts to disable the seal with an electronic signal. This method fails because there are no electronic connections to the seal.
- The attacker cuts the test fiber, accesses the sealed component, and attempts to replace the fiber seal. This method fails for multiple reasons. First, the attacker would have to know the length of the fiber accurate to 10 microns; he has no way of determining the length at all. Second, the fiber is connected inside the enclosure, which is also sealed. He would have to access the enclosure first, which would destroy the reference fiber. Finally, the attacker would have to produce a replacement fiber of exactly the same length (and optical material) and then re-insert it.
- The attacker attempts to clone the entire seal system (fiber, optics, and electronics) and then tries to substitute it. This attack fails for multiple reasons. First, there is no way that the attacker can learn about the exact lengths of the fibers. Any attempt would destroy them. Second, if these systems are monitored, which only makes sense for an active seal, then the replacement attempt would be detected immediately.

B. Switched Active Seal

The second seal variant we have designed is a switched active seal. The motivation for this seal design is purely cost. If we consider the cost of fully fabricated system components as shown in Figure 2 above, the components in the “green” and “grey” could be fabricated and sold commercially for nominally $500, and probably less. The fibers themselves would cost only a few pennies. Most of the cost would be labor. However, the cost for the electronic and optical components in the “brown”, for example, the pulsed laser, the computer, and the spectrometer, would nominally cost $50,000, or about 100 times more. The design of the switched active seal is intended to reduce the overall per seal cost by an inverse factor of roughly the number of seal units. The topology is shown below in Figure 5.

This design has only a single electronics / optical unit consisting of the expensive components (laser, computer, fiber switch, and spectrometer). The individual seal units consist of just the test and reference fibers, their container, the optical coupler, and the encrypted optical switch; all are relatively inexpensive. The fiber switch switches the laser light and spectrometer between the individual seals. This switch preserves both phase and polarization of the laser light in the single mode fibers. It is controlled by the system computer, so that each seal can be interrogated by the laser pulse a programmable number of times before the computer switches to the next seal. To appreciate the time scales involved, consider a 100 MHz laser pulse rate and an interrogation time of 1 second per seal. Then a room of 100 canisters could be fully interrogated in 100 seconds. The system would operate continuously and return to the first canister, so that every container would be interrogated every 100 seconds.

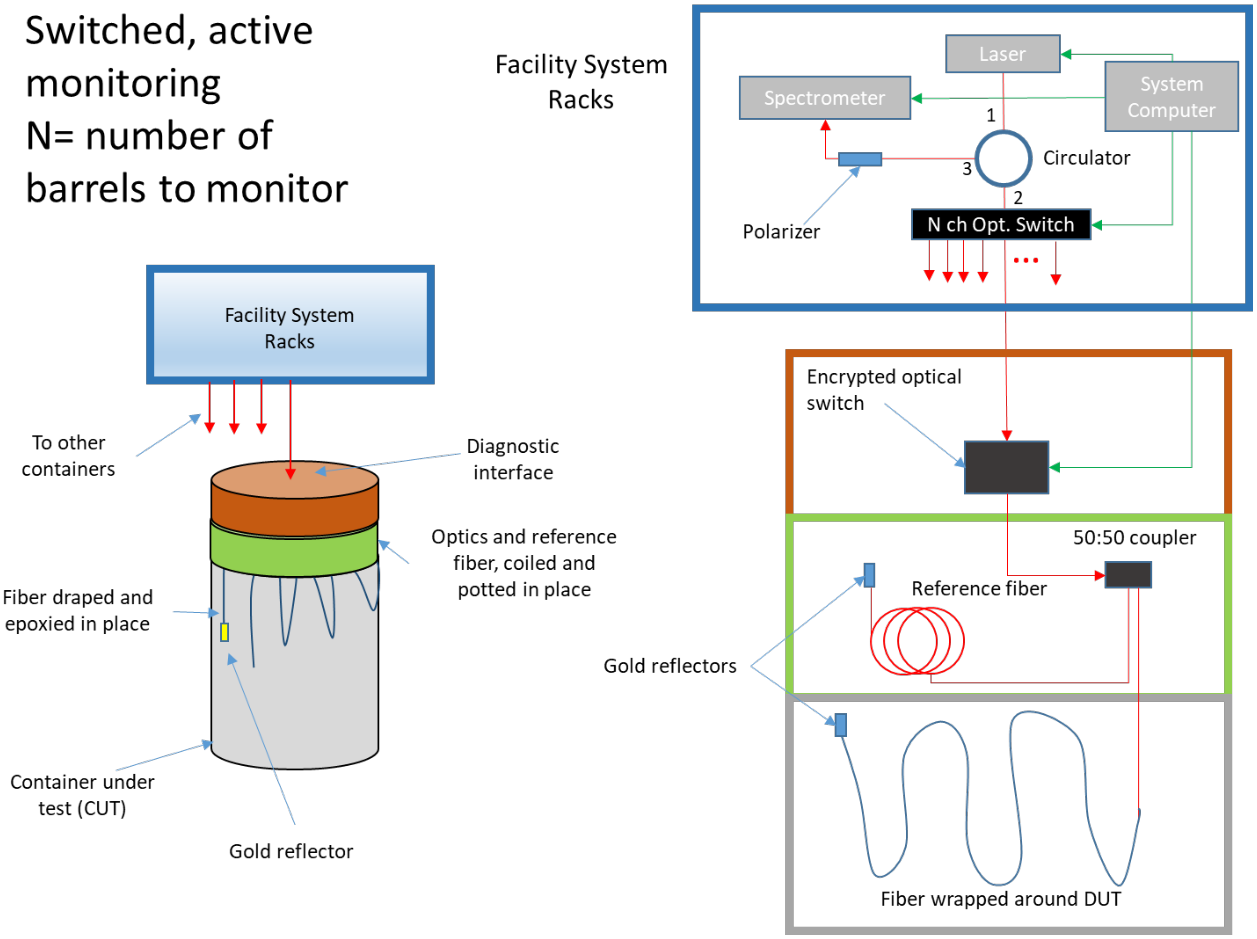

Figure 5: System design for the switched active seal variant of the spectral interference seal. Not that only the inexpensive component, (i.e. the two fibers, the optical coupler, and the seal container), is repeated for each seal. The expensive components consisting of the laser, the spectrometer, the computer, and the circulator are used only once. This design adds two other components: a multi-channel optical switch and an encrypted optical switch. The multi-channel optical switch switches between each of the individual fiber seals.

A new aspect of this design is the encrypted optical switch. The purpose is to optically disconnect the seal fibers from the outside when they are not being interrogated. It provides another layer of protection by preventing an attacker from optically accessing the seal. Although the overall scenario is quite unlikely, without this switch an attacker could use something like a LUNA^{TM} Swept Wavelength Reflectometer to interrogate both the reference and test fibers and determine their lengths. However, even if this were possible, the attacker would then have to be able to construct a fiber pair with an optical length difference accurate to only 10 microns, and would have to be able to substitute those fibers for the original seal undetected. That would have the same difficulties as discussed for the active seal: it would require access to the seal enclosure, which is protected by the reference fiber epoxied in place. However, the encrypted optical switch prevents even this scenario.

The encrypted optical switch consists of an ordinary, phase-preserving switch similar to the N-channel fiber switch discussed above. It works by standard asymmetric cryptography. The optical switch would be connected to a simple micro-controller programmed with commercial-quality encryption, such as the RSA family of algorithms. The private key for asymmetric encryption would be stored only on the system computer; the encrypted optical switch for each of the individual seals would contain the public key. The system computer would provide the private key to the encrypted optical switch, which would compare to the public key in its storage. If a match were made, the micro-controller would enable the optical switch to allow the system to access the seals and perform the interrogation.

The bench-top test system shown in Figure 3 above and discussed in Section II.A actually implemented a simple form of the switched active seal. The fiber-coupled interferometer was switched between three separate test fibers. The process was identical to that discussed above; the switch would interrogate each of the fibers and then repeat the sequence. Each individual test fiber was interrogated for a nominal 2,000 pulses before the system switched to the next fiber in the sequence. For each test pulse, the FFT of the raw data provided the differential fiber length, as shown in Figure 4 above. The summary results of all 10,000 tests is plotted below Figure 6. The important observation from these results is the measurement precision. As can be seen from the plot, the nominal variance for the measurements is about 25 microns. With a more resolved spectrometer, and including the statistics for multiple tests (i.e. multiple FFT reduced downloaded spectra), this variance should be no more than 10 microns.

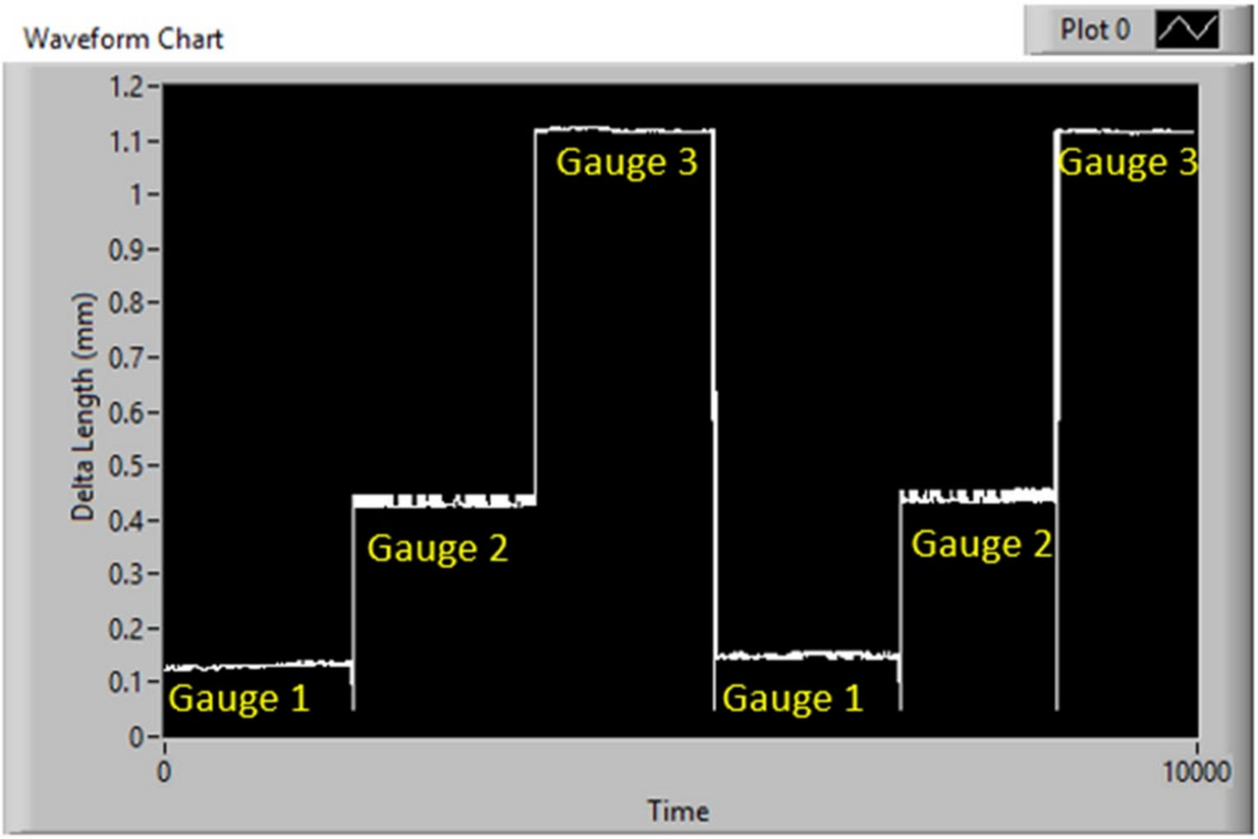

Figure 6: Results from the bench-top system using an optical switch and three different test fibers. This plot shows the optical length difference between three different test fibers and a single reference fiber. The system automatically switches between the three test fibers and then repeats the sequence. This mimics closely the method of the switched active seal.

1. Initial Vulnerability Assessment for This Configuration

The vulnerability issues with this alternative configuration is largely the same as for the active seal version, so we will only discuss the differences. These are:

- The length of time between interrogations has increased from nominally 1 microsecond to 100 seconds. However, this is not significant because the real strength of the seal is the difficulty (near impossible) of cloning the seal to the required 10 micron accuracy. That technology does not exist.
- An attacker could attempt to access the optical port when the seal was not being interrogated, and use a device such as a LUNA^{TM} Swept Wavelength Reflectometer to determine the lengths of both Michelson fibers. This attack would fail for several reasons. First, the attacker would have to time the measurement for a period when the seal was not being interrogated, but he would not know which seals are being interrogated at any time and in what order. Second, even knowing this information, he would have to fabricate a cloned seal with an accuracy of 10 microns. And, with that cloned seal, replace the existing seal in its entirety during a period when the seal was not being actively interrogated. Third, we have added an encrypted optical switch to the optical circuit. That switch prevents optical access to the interferometer unless a private key is provided, (using asymmetric cryptography). Without that key, the attacker could not gain access to make the measurement. We maintain that asymmetric cryptography is very robust, as it is the basis for world-wide banking. Finally, it takes much longer than 100 seconds to perform a fiber splice. Our experience is that 5 to 10 minutes is typically required, and that is if the length is already known. The strength of the seal is that it has these multiple safeguards in combination.

C. Passive Seal

The final configuration for the spectral interference seal is a passive configuration. This design is very similar to the switched active seal discussed in Section II.B and shown in Figure 5 above. The passive seal design is shown below in Figure 7. This seal variant is very similar to the switched active seal. The major difference is that rather than switching actively and continuously, the seal is interrogated with a portable laser interferometer system that would be hand-carried by an inspector during a routine inspection. The inspector would connect the laser interferometer unit to the individual seal and the system would make the measurement (which would consist of nominally a thousand separate laser pulse interrogations. The average would be compared to the previous measurement stored on the interrogating unit computer. The inspection frequency would be determined by the normal inspector visit frequency to a facility.

The principle benefit of the passive seal design is cost. The cost of the individual seal itself would nominally be about $200. The expensive components, (i.e. the spectrometer, laser, circulator, computer), would be contained entirely in the Portable Test System, which could service an essentially unlimited number of seals.

A modest variant of this seal would be to store the spectrum and the FFT of the spectrum (ref. Figure 4 above) in the encrypted optical switch. The encrypted optical switch would consist of a standard telecommunications optical switch powered by, say a Microchip ATSAMD51 microcontroller implemented on an Adafruit ItsyBitsy M4 Express microcard ($15) with 2MB of flash storage. This chip could store the spectrum and FFT of the spectrum and would use the same private key, asymmetric cryptography, protected access as for opening the optical switch. Using this approach, the specific spectral interferogram is stored on the seal itself; it would not be necessary to store it on the interrogating system.

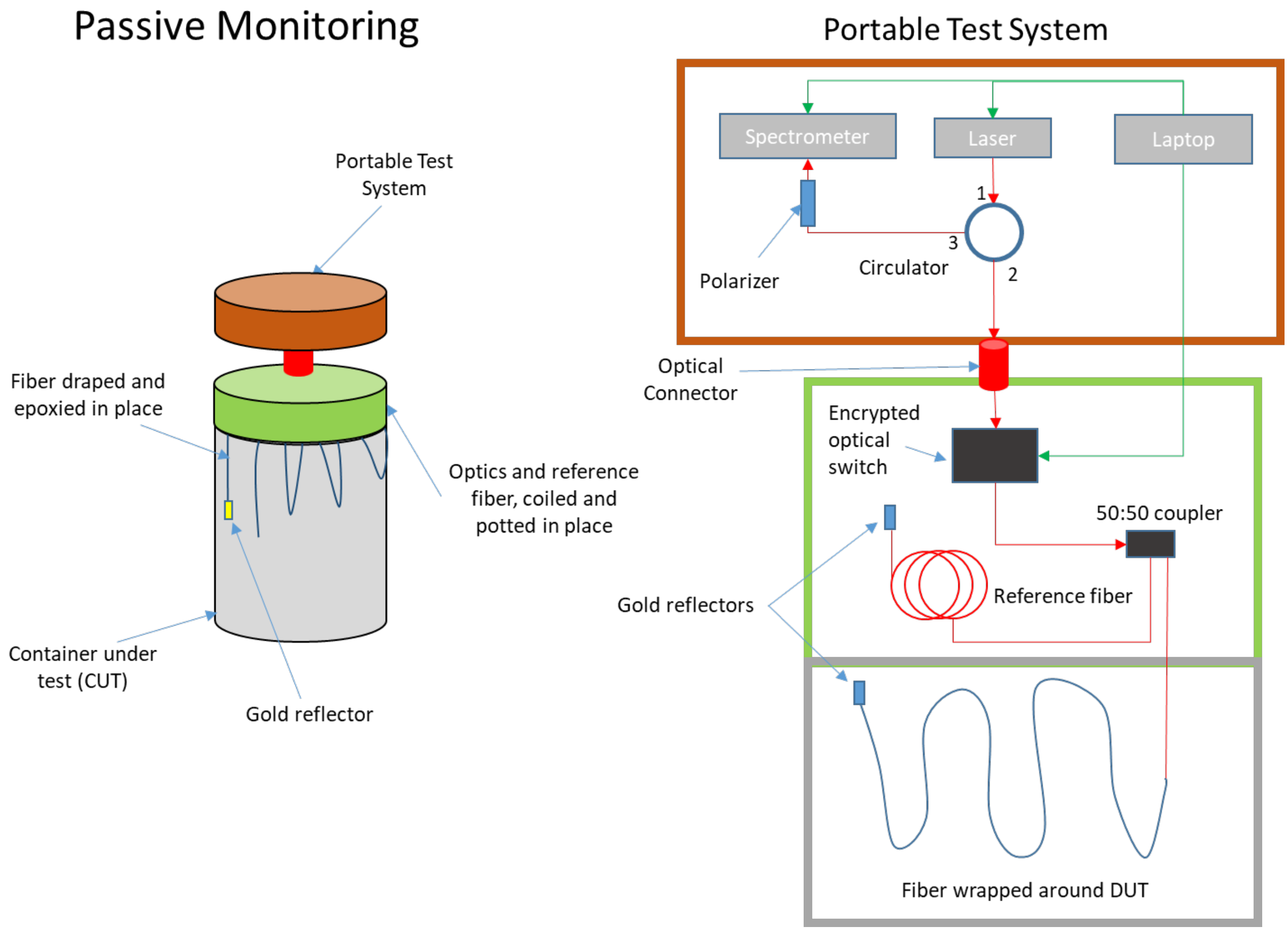

Figure 7: Optical and electronic schematic of the passive variant of the spectral interference seal. The components are the same as the diagrams above. This is most similar to the

III. Next Step

The next step will be to purchase parts selected properly for this application. In particular, we will purchase a higher resolution spectrometer. We will then construct a compact instrument of the type shown above in Figure 2, namely an active system. Such a system would be the best for demonstration purposes. This system will be properly engineered and compact. We will put it in a small Pelican type container, so that it could be taken to potential sponsors and demonstrated.